UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
GREENBELT DIVISION

PATI SPRINGMEYER, an individual and Nevada Resident, and JOE LOPEZ, an individual and California Resident, on behalf of themselves and all others similarly situated, Plaintiffs, v. MARRIOTT INTERNATIONAL, INC., a Montgomery County, Maryland Resident, Defendant.	Case No. 8:20-cv-00867-PWG Judge Paul W. Grimm

BRIEF IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS PLAINTIFFS' FIRST AMENDED COMPLAINT

Paul B. Rietema (*pro hac vice*)
Jenner & Block LLP
353 N. Clark St.
Chicago, Illinois 60654
Telephone: (312) 840-7208
Facsimile: (312) 840-7308
prietema@jenner.com

David W. DeBruin (Bar No. 07757)
Lindsay C. Harrison (*pro hac vice*)
Zachary C. Schauf (*pro hac vice*)
Jenner & Block LLP
1099 New York Ave. NW, Suite 900
Washington, DC 20001
Telephone: (202) 639-6865
Facsimile: (202) 639-6066
ddebruin@jenner.com
lharrison@jenner.com
zschauf@jenner.com
Attorneys for Defendant

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTRODUCTION

Plaintiffs Pati Springmeyer and Joe Lopez ("Plaintiffs") bring a nationwide putative class action against Marriott International, Inc. ("Marriott") over a recent incident in which "two employees at a [Marriott] franchise" in Russia "improperly accessed" certain guest information. First Am. Compl. ("FAC" or "Complaint") ¶ 23. Plaintiffs do not claim in this case that Marriott's systems were "hacked" or left vulnerable to attack by outsiders. Nor do they claim that the improper access affected social security numbers, credit card information, passport information, or other similarly sensitive information. Nor, finally, do Plaintiffs allege that the information that was accessed has actually been *used* in any way, much less *mis*used. Under these circumstances, Plaintiffs lack Article III standing to sue—one of several fatal defects in their Complaint.

The Fourth Circuit's rule is that "a mere compromise of personal information … fails to satisfy [Article III's] injury-in-fact element" "in the absence of an identity theft." *Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc.*, 892 F.3d 613, 621 (4th Cir. 2018). This rule enforces the bedrock principle that federal courts lack jurisdiction when plaintiffs allege only that they *may someday* be injured. Only when an injury has occurred, or is "certainly impending," is there an Article III "case or controversy." *Beck v. McDonald*, 848 F.3d 262, 274-75 (4th Cir. 2017).

Plaintiffs allege no more than "mere compromise." They do not claim their information (or anyone's) has been misused. Nor do they plausibly allege an imminent threat of misuse. The incident affected only information "such as names, addresses, phone numbers, birthdays, loyalty information." FAC ¶¶ 23-24. Such information is often voluntarily disclosed, is widely available on the internet, and frequently is *required* to be disclosed by public-records laws.[1] Springmeyer's

[1] For example, land records containing names and addresses are publicly available. Nev. Rev. Stat. Ann. § 111.312; Cal. Gov't Code § 27321.5. In fact, this Court's local rules require that the case caption on an original complaint "contain the names and addresses of all parties" and that "any

address, for example, is available from Whitepages.com and Fastpeoplesearch.com; her email and phone number are posted on her own Facebook pages; and her birthday is posted on an art page.[2] While Plaintiffs say that *in general* "personal identifiable information" (or "PII") can be used to access "accounts and … effectuate identity theft," FAC ¶ 42, they allege no facts showing that the disclosure of the *type of PII* at issue here creates an imminent risk *to these Plaintiffs*.

Plaintiffs cannot plead around *Hutton* and *Beck*. They insist they are at "increased risk of fraud and identity theft" and have "pa[id] … for credit monitoring." FAC ¶¶ 15, 20. *Hutton* and *Beck*, however, rejected identical arguments. Plaintiffs say their information has diminished in value, and that they lost the benefit of their bargain. *Id.* But Plaintiffs allege no facts showing that their "names," "addresses," and "birthdays" have decreased in value. Nor do they plausibly allege that they would have paid less, or not booked, had they known this information was at risk of improper access by franchise employees (who, after all, generally are *expected* to access such guest data for individual bookings). In fact, the very privacy statement Plaintiffs rely upon explains that, while Marriott "seek[s] to use reasonable … measures," "no data … system" is "100% secure" and "compromise[s]" are possible.[3] Finding standing here would conflict with not only *Hutton* and *Beck*, but with *In re Marriott International, Inc., Customer Data Security Breach Litigation*, 440 F. Supp. 3d 447, 455, 459-60 (D. Md. 2020).

---

pleading seeking to add a new party … contain … the name and address of the parties sought to be added," MD R USDCT Civ Rule 102, though Plaintiffs have failed to comply with this Rule.

[2] https://www.whitepages.com/address/2817-Cotton-Cloud-Rd/Las%20Vegas-NV/3qU6Z4J244hdbSsTQhCVr1; https://www.fastpeoplesearch.com/name/pati-springmeyer; https://www.facebook.com/pati.springmeyer; https://www.facebook.com/seasonalcolorstudio/; https://www.facebook.com/pg/Bourbon-Couture-1542449762697781/; https://www.deviantart.com/patispringmeyer.

[3] Marriott Group Global Privacy Statement as of Mar. 20, 2020, http://web.archive.org/web/20200328180639/https://www.marriott.com/about/privacy.mi. On a motion to dismiss, a court may "consider documents that are explicitly incorporated into the complaint by reference." *Goines v. Valley Cmty. Servs. Bd.*, 822 F.3d 159, 166 (4th Cir. 2016).

Even if Plaintiffs had standing, the Complaint would have to be dismissed because they have not adequately pled their causes of action. Among many other defects, all Plaintiffs' claims fail because they do not plausibly plead what Marriott's security procedures were or how they were deficient. The conclusory assertion that Marriott "fail[ed] to implement … reasonable cyber-security procedures," FAC ¶ 5, mocks the requirements of *Iqbal* and *Twombly*. Finally, any putative classes would in any event need to be limited to Nevada and California, where Plaintiffs reside. For these reasons and others, the Complaint must be dismissed.

BACKGROUND

On March 31, 2020, Marriott notified 5.2 million guests that "two employees at a [Marriott] franchise" had "improperly accessed" certain information. FAC ¶ 23. Marriott explained it had discovered "[a]t the end of February 2020" that "an unexpected amount of … information may have been accessed … start[ing] in mid-January 2020." *Id.* ¶ 24. "Upon discovery," Marriott "confirmed that the login credentials were disabled, … began an investigation, implemented heightened monitoring, and arranged resources to inform and assist guests." *Id.* ¶¶ 23-24. The information included contact details like "name, mailing address, [and] email address," personal details like "gender, and birthday day and month," and "[l]oyalty [a]ccount [i]nformation," such as "account number and points balance." *Id.* Marriott had "no reason to believe" the information included "passwords or PINs, payment card information, passport information, … or driver's license numbers." *Id.* Still, Marriott offered "one year of free" monitoring. *Id.* ¶ 71.

On April 1, 2020, Pati Springmeyer filed this putative class action. Dkt. 1. After Marriott filed its pre–motion-to-dismiss letter, Dkt. 31, Springmeyer amended and added plaintiff Joe Lopez. Neither, however, claims their information has been misused. They assert that they suffered "actual injury" from "increased risk of fraud and identity theft"; from monitoring costs; from their information's diminished "value"; and from losing the benefit of their bargain. *Id.* ¶¶ 15, 20. The

Complaint includes 11 counts. Plaintiffs purport to represent a nationwide class, claiming Maryland law governs the common-law claims. *Id.* ¶ 94. Alternatively, they seek to represent classes for their states of residence (Nevada for Springmeyer, California for Lopez). *Id.* ¶¶ 78-79.

STANDARD OF REVIEW

Under Rule 12(b)(1), plaintiffs bear the burden of establishing subject-matter jurisdiction. *Demetres v. E. W. Constr., Inc.*, 776 F.3d 271, 272 (4th Cir. 2015). In assessing a Rule 12(b)(1) challenge to standing, courts accept factual allegations as true but "do not [ ] apply the same presumption of truth to 'conclusory statements.'" *Beck*, 848 F.3d at 270. Under Rule 12(b)(6), plaintiffs must establish "facial plausibility" by pleading "factual content that allows the court to draw the reasonable inference that the defendant is liable"; "[t]hreadbare recitals …, supported by … conclusory statements, do not suffice." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

ARGUMENT

I. Plaintiffs Lack Article III Standing.

Plaintiffs lack Article III standing. The "irreducible constitutional minimum" of standing is that a plaintiff must have suffered an "injury in fact" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Beck*, 848 F.3d at 269; *see Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). This injury also must be "fairly traceable" to the challenged conduct, and likely to be redressed by a favorable decision. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013). Here, Plaintiffs have not pled either injury-in-fact or traceability.

A. Plaintiffs Have Not Alleged An Injury-in-Fact.

Plaintiffs do not claim their identities have been stolen, that they suffered fraud, that their loyalty points have diminished, or that their information has been misused. They sued after ordinary information—"names, addresses, phone numbers, birthdays, loyalty information," but not "passwords …, payment card information, passport information, … or driver's license numbers"—

was "improperly accessed." FAC ¶¶ 23-24. This case thus raises the question whether an individual incurs Article III injury whenever *any* personal information is accessed without authorization.

In the Fourth Circuit, the answer is clear: "[M]ere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft." *Hutton*, 892 F.3d at 621. In *Beck*, sensitive personal information including "social security numbers" and "medical diagnoses" was compromised—yet plaintiffs lacked standing because the information had not been "misused" or led to "identity theft." 848 F.3d at 267-68, 274. *Beck* distinguished cases finding standing in data-breach cases on the ground that "at least one named plaintiff alleged misuse." *Id.* at 274. *Hutton* considered the opposite situation and found standing because the plaintiffs alleged not just that "social security numbers … and credit card information" was "stolen" and "accessed," but that they had been "used in a fraudulent manner." 892 F.3d at 622.

Likewise, *In re Marriott* found standing after this Court concluded that the complaint "extensive[ly] alleg[ed]" "targeting of" sensitive information including "passport" and "payment card numbers … for misuse," and "actual misuse by some" named plaintiffs. 440 F. Supp. 3d at 459. While Marriott disagrees that standing existed in that case, *In re Marriott* supports dismissal here—where neither Plaintiff alleges misuse and the information was not sensitive.

Plaintiffs' several attempts to plead around *Beck*, *Hutton*, and *In re Marriott* each fail.

1. Absent Misuse, Plaintiffs Cannot Manufacture Standing By Claiming "Increased Risk of Identity Theft" Or By Voluntarily Spending Money.

First, Plaintiffs claim that the incident put them at "increased risk of fraud and identity theft," and that they spent money to mitigate that risk. FAC ¶¶ 15, 16.

The Fourth Circuit has rejected those exact arguments. It "reasoned in *Beck* that a plaintiff fails to 'establish Article III standing based on the harm from the increased risk of future identity theft and the cost of measures to protect against it.'" *Hutton*, 892 F.3d at 621. That is because,

when plaintiffs ground standing on a risk of future injury, the "threatened injury must be certainly impending." *Beck*, 848 F.3d at 272. But when plaintiffs allege only "mere compromise," any "'enhanced risk of future identity theft' is 'too speculative.'" *Hutton*, 892 F.3d at 621. Before the plaintiffs would suffer genuine harm, an "attenuated chain of possibilities" must come to pass: The court must "assume that [a] theft targeted the stolen items for" identity theft; that a thief then "select[s], from thousands [or millions] of others, the personal information of the named plaintiffs"; that the information the thief has acquired is *sufficient* to effect identity theft; and that the thief successfully "use[s] that information to steal [the named plaintiffs'] identities." *Beck*, 848 F.3d at 275. This speculative chain did not confer standing in *Beck*, and it cannot here. *Accord Kimbriel v. ABB, Inc.*, No. 19-CV-215, 2019 WL 4861168, at *3 (E.D.N.C. Oct. 1, 2019) (even when "credit inquiries" appeared after a "targeted hack," the risk was "still too speculative").

In fact, Plaintiffs' claims are far *weaker* given the type of information at issue here. Plaintiffs belabor the point that *in general* "[i]dentity thieves can use personal information … to perpetrate a variety of crimes that harm victims." FAC ¶ 58; *see id.* ¶¶ 42-43, 46-47. But this case concerns common information like "names, addresses, phone numbers, birthdays, loyalty information," FAC ¶ 23, which people like Springmeyer routinely disclose publicly. Not a single well-pled allegation plausibly shows that access to this sort of personal information renders identity theft "certainly impending." Courts routinely find standing lacking in cases about the disclosure of such information. *See, e.g.*, *Stasi v. Inmediata Health Grp. Corp.*, No. 19CV2353, 2020 WL 2126317, at *5 (S.D. Cal. May 5, 2020) (plaintiffs failed to plead theft of "social security numbers, or similarly sensitive financial or account information").[4]

[4] *Accord Brett v. Brooks Bros. Grp., Inc.*, No. CV 17-4309, 2018 WL 8806668 (C.D. Cal. Sept. 6, 2018) (payment card numbers, expiration dates, verification codes); *Antman v. Uber Techs., Inc.*, No. 15-cv-01175, 2018 WL 2151231, at *10 (N.D. Cal. May 10, 2018) (names, driver's license

Also insufficient is Springmeyer's claim that she spent money to mitigate her perceived risk, particularly where Marriott has already offered her one year of free monitoring. FAC ¶¶ 15, 71. *Beck* found that mitigation costs "did not constitute injury-in-fact when the threat … was too speculative." *In re Marriott*, 440 F. Supp. 3d at 460; *see Beck*, 848 F.3d at 276-77. That is, "the two theories of injury-in-fact stand or fall together." *In re Marriott*, 440 F. Supp. 3d at 460.

2. Plaintiffs Cannot Plead Around *Hutton* And *Beck* With Conclusory Assertions Of "Diminished Value" Or Lost "Benefit Of Their Bargain."

Plaintiffs cannot avoid dismissal by claiming that, when two franchise employees accessed their information in Marriott's systems, their information diminished in value or they lost the benefit of their bargain. FAC ¶¶ 15, 20. Accepting either theory, on these facts, would yield the result *Hutton* and *Beck* rejected: standing based on "mere compromise of personal information."

Diminished value. Although Plaintiffs generically allege that their personal information's "value" has "diminished," FAC ¶ 142, they proffer no facts supporting that claim. "All victims of security breaches" can raise boilerplate claims of "diminution of … value." *Kimbriel*, 2019 WL 4861168, at *3. "Were it the case that these harms constituted injury-in-fact, all victims … would satisfy [that] requirement"—which "is foreclosed by precedent." *Id*. (citing *Beck*).

This failure is especially telling given *In re Marriott*, which found that plaintiffs could proceed if they showed harm to "the economic benefit [a] consumer derives from being able to [make] purchase[s] remotely and without the need to pay in cash or a check." 440 F. Supp. 3d at 462. That was the only basis on which this Court "depart[ed] from" *Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564, 572 (D. Md. 2016), and *Khan v. Children's National Health System*, 188 F. Supp. 3d 524, 533-34 (D. Md. 2016), which rejected "diminished value" claims. Yet Plaintiffs do

numbers); *Green v. eBay Inc.*, No. CIV.A. 14-1688, 2015 WL 2066531, at *4 (E.D. La. May 4, 2015) (names, encrypted passwords, birthdays, emails, addresses, phone numbers).

not allege they have become less able to engage in online commerce. So while Marriott again does not agree with *In re Marriott*, that decision underscores that this case must be dismissed. *Accord Green v. eBay Inc.*, No. CIV.A. 14-1688, 2015 WL 2066531, at *5 n.59 (E.D. La. May 4, 2015) ("Even if … personal information … has an inherent value … Plaintiff has failed to allege facts indicating how the value … has decreased as a result of the Data Breach.").

It is no mystery why such allegations are absent in this case. In *In re Marriott*, and in every case it cited as "recogniz[ing] the lost property value of [personal] information," 440 F. Supp. 3d at 461, the personal information at issue was either social security numbers or credit card numbers. *Id.* at 454-55, 459.[5] Not so here. This case is like *Chambliss*, which involved "only … names, birthdates, email addresses, and subscriber identification numbers," not "social security numbers, credit card information, or … similarly sensitive data." 189 F. Supp. 3d at 570.

Overpayment. Plaintiffs' "overpayment" theory—*i.e.*, that they "pa[id] monies to Marriott … which [otherwise they] would not have"—fails for similar reasons. FAC ¶¶ 15, 20. True, Plaintiffs *assert* they "pa[id] monies to Marriott … which [they otherwise] would not have." FAC ¶¶ 15, 20. But "[t]hreadbare recitals," and "mere conclusory statements, do not suffice." *Lombel v. Flagstar Bank F.S.B.*, No. 13-704, 2013 WL 5604543, at *3 (D. Md. Oct. 11, 2013) (quoting *Iqbal*, 556 U.S. at 678). Plaintiffs must "plead[] factual content that allows the court to draw [a] reasonable inference" that they lost the benefit of some bargain. *Id.* While the Court found the allegations *In re Marriott* sufficient, 440 F. Supp. 3d at 465-66, here they fall short.

First, it is one thing to find that plaintiffs may have lost the benefit of some bargain where

[5] *In re Experian Data Breach Litig.*, No. CV151592, 2016 WL 7973595 (C.D. Cal. Dec. 29, 2016); *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617, 2016 WL 3029783 (N.D. Cal. May 27, 2016); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752, 2017 WL 3727318, at *13 (N.D. Cal. Aug. 30, 2017). The Court also cited *In re Facebook Privacy Litig.*, 572 F. App'x 494 (9th Cir. 2014), but that unpublished decision did not address Article III standing.

sensitive information like payment cards and passports were allegedly compromised *and misused*. It is another, and irreconcilable with *Hutton* and *Beck*, to do so when plaintiffs allege only "mere compromise" of non-sensitive information—particularly when the compromise came via franchise employees' credentials that are intended to access guest contact information of the type involved here. 892 F.3d at 621.

Second, the Complaint is bereft of any facts plausibly alleging that Marriott's data security practices for franchise employees mattered in where Plaintiffs booked or what they paid. Plaintiffs do not even allege that they read Marriott's Privacy Statement before booking in order to compare the details of Marriott's practices with those of other hotel companies. Certainly, Plaintiffs plead no facts suggesting that they would have gone elsewhere—or have been able to pay less—had they known information such as their name and email might be "improperly accessed" (but not misused), much less by hotel employees who, generally, have access to such data. *Id.* ¶ 3. Indeed, they plead no facts showing that *any* hotel has given a discount because a guest raises concerns about any aspect of data security. While guests may of course choose alternative hotels, Plaintiffs themselves allege that breaches are "prominen[t]" in the "hospitality industry" generally. *Id.* ¶ 100.

Third, Plaintiffs have not pled "an explicit or implicit contract for data security"—as detailed below. Part II.C; *cf. In re Marriott*, 440 F. Supp. 3d at 466. Plaintiffs rely on Marriott's "Global Privacy Statement." FAC ¶ 35. But even if that were a binding contract, it provides only that Marriott "*seek*[*s*] *to* use reasonable [security] measures," and—in language Plaintiffs omit—cautions that "[u]nfortunately, no data transmission or storage system can be guaranteed to be 100% secure" and "compromise[s]" are possible. This is not a promise that no unauthorized access will occur. *Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 717 (8th Cir. 2017) (rejecting "benefit of the bargain" theory where defendant did not "promise[] that its customer data would not be hacked");

Jackson v. Loews Hotels, Inc., CV18-827, 2019 WL 6721637, at *2 (C.D. Cal. July 24, 2019) (same, where policy "put consumers on notice that … data security practices are not bulletproof"). Nor is it a promise that Marriott will implement any particular measures. *In re Vale S.A. Sec. Litig.*, No. 15-CV-9539, 2017 WL 1102666, at *21 (S.D.N.Y. Mar. 23, 2017) (statements of what a company "seek[s]" to do are "aspirational" and "consistently held to be inactionable").

Fourth, even had Marriott promised "reasonable" security practices, Plaintiffs have not plausibly pled a breach. Again, they *assert* that Marriott "fail[ed] to implement … reasonable" procedures, FAC ¶ 5, but they plead no *facts* rendering that assertion plausible. *See infra* Part II.B.1. Plaintiffs simply intone that Marriott fell short of "reasonable" practices. FAC ¶¶ 5, 6, 53, 87(g), 87(h), 101, 102, 103, 108, 112, 127, 150(c), 181, 184, 191(a), 191(d). In *Kuhns*, the Eighth Circuit upheld dismissal of a complaint containing similar allegations that the defendant lacked "sufficient security measures," explaining that "we are left to guess how" the measures were deficient. 868 F.3d at 718; *see Attias v. CareFirst, Inc.*, 365 F. Supp. 3d 1, 13 (D.D.C. 2019) (similar), *appeal docketed*, No. 19-7020 (D.C. Cir. Mar. 14, 2019). By contrast, in each case *In re Marriott* cited as recognizing a benefit-of-the-bargain theory, plaintiffs alleged concrete facts stating *how* defendants fell short. *See Carlsen v. GameStop, Inc.*, 833 F.3d 903 (8th Cir. 2016) (sharing information with third parties in violation of policy); *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 985 (N.D. Cal. 2016) (failing to take specific measures advised by the federal government); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752, 2017 WL 3727318, at *13 (N.D. Cal. Aug. 30, 2017) (safeguards violated federal regulations).

In short, this case could not be more different from benefit-of-the-bargain cases finding standing. It does not concern a failure to prevent an outside hack, and Plaintiffs have yet to identify any way that Marriott's security practices fell short. Plaintiffs do not plausibly allege that anyone

books a hotel room assuming that hotel employees will not access their information. That is particularly true of the common contact information at issue here, which is generally *already* widely available. While the franchise employees here may have accessed information for *more* individuals than was permitted, that does not deprive Plaintiffs of the benefit of their bargain.

B. Plaintiffs Have Not Alleged That Any Injury Is Fairly Traceable To The Conduct Of Which They Complain.

Similarly, Plaintiffs have not pled that any injuries are "fairly traceable to the challenged action." *Bishop v. Bartlett*, 575 F.3d 419, 423 (4th Cir. 2009). The "challenged action" is Marriott's supposed "failure to implement … reasonable cyber-security procedures." FAC ¶ 5. But again, Plaintiffs plead no facts identifying how some hypothetical "reasonable" procedures (which they have yet to identify) would have avoided improper access by franchise employees. *See Anderson v. Kimpton Hotel & Rest. Grp.*, LLC, No. 19-CV-01860, 2019 WL 3753308, at *3-4 (N.D. Cal. Aug. 8, 2019) (standing absent where plaintiff failed to "allege the nature of any assertedly reasonable, appropriate, obligatory, sufficient and/or adequate action [defendant] failed to take").

C. Plaintiffs Lack Standing For Injunctive Relief

Plaintiffs also lack standing to seek injunctive relief. "A plaintiff who seeks ... to enjoin a future action must demonstrate that he 'is immediately in danger of sustaining some direct injury.'" *Beck*, 848 F.3d at 277. The *Beck* plaintiffs sought injunctive relief on the ground that they had suffered at least two data breaches from the defendant's systems, that the defendant allegedly had "never been in compliance" with applicable data safeguards, and that the defendant allegedly would "[n]ever achieve compliance … left to its own devices." *Id.* Standing was absent, however, because those allegations only raised the possibility that the plaintiffs "could" be affected by another breach, not an immediate danger. *Id.* Here, Plaintiffs' allegations fall far short even of what *Beck* deemed insufficient. FAC ¶¶ 151-154. Hence, Plaintiffs lack standing.

II. Plaintiffs Fail To State A Claim Upon Which Relief Can Be Granted.

Even if Plaintiffs had standing, none of the Complaint's 11 counts states a claim.

A. The Common-Law Claims Are Governed By Nevada And California Law.

Plaintiffs initiated this action in Maryland, so Maryland's choice-of-law rules control. *Bank of La. v. Marriott Int'l, Inc.*, 438 F. Supp. 3d 433, 441 (D. Md. 2020). Plaintiffs allege that Maryland law applies to their purportedly "nationwide" common law claims. FAC ¶ 94. But consistent with *In re Marriott*, such claims will be governed by the laws of the Plaintiffs' residences—Nevada for Springmeyer and California for Lopez. 440 F. Supp. 3d at 442-43.

For the tort claims (Counts 1, 2, 5, 7), "the *lex loci delicti* rule" governs. *Smith v. MTD Prod., Inc.*, No. CV 19-1592, 2019 WL 5538273, at *2 (D. Md. Oct. 24, 2019) (citing *Proctor v. Wash. Metro. Area Transit Auth.*, 412 Md. 691, 726 (2010)). Under that rule, "the substantive tort law of the state where the wrong occur[s]" governs. *Philip Morris Inc. v. Angeletti*, 358 Md. 689, 744 (2000). "[W]here the events giving rise to a tort action occur in more than one state, the court must apply the law of the State where the injury … occurred." *Bank of Louisiana*, 438 F. Supp. 3d at 442. Here, any injury would have been felt in Plaintiffs' states of residence. *See id.* at 443.

For the contract claims (Counts 3, 4), "the '*lex loci contractus*' principle" governs, and "'the law of the jurisdiction where the contract was made controls.'" *Noohi v. Toll Bros.*, 708 F.3d 599, 607 (4th Cir. 2013) (quoting *Kramer v. Bally's Park Place, Inc.*, 311 Md. 387, 390 (1988)). A contract was "made" where "the last act necessary … is performed." *Encompass Home & Auto Ins. Co. v. Harris*, 93 F. Supp. 3d 424, 432 (D. Md. 2015). Any alleged contract would have been accepted, and so "made," in Plaintiffs' home states.

B. Plaintiffs' Negligence And Negligence *Per Se* Claims Fail.

Plaintiffs' first and second claims—for negligence and negligence *per se*—both fail.

1. Plaintiffs Have Not Pled Negligence Or Negligence *Per Se.*

The elements of negligence are (1) "a duty," "(2) breach of that duty, (3) legal causation, and (4) damages." *Sanchez ex rel. Sanchez v. Wal-Mart Stores, Inc.*, 125 Nev. 818, 824 (2009); *see Paz v. Cal.*, 22 Cal. 4th 550, 559 (2000). Negligence *per se* (where it exists) requires the same elements, but a statute defines duty and breach. *Sanchez*, 125 Nev. at 828.

The Complaint fails to satisfy these elements. First, Plaintiffs do not plausibly allege duty or breach. They assert that Marriott had a duty to take "reasonable care in safeguarding" their information, and breached that duty by failing to implement "adequate" security measures or abide by FTC "publications." FAC ¶¶ 96, 101-102, 111-112. But again, they plead no facts supporting these assertions. The complaint contains no allegations about *what* Marriott's security practices were, or *how* they were inadequate. *See* FAC ¶ 53 (assertion that failure to employ "reasonable … measures" was an "unfair act or practice prohibited by" FTC Act); *cf. Anderson*, 2019 WL 3753308, at *5 (dismissing because allegations that defendant "failed to act in a 'reasonable' … manner and failed to take … 'adequate' steps to protect plaintiffs' PII" were "conclusory").

At bottom, Plaintiffs imply that unauthorized access *itself* is sufficient to plead that Marriott's security was deficient. *E.g.*, FAC ¶ 101. That is precisely the argument properly rejected in *Kuhns*, which explained that the plaintiffs' "implied premise"—that "because data was hacked … protections must have been inadequate"—is a "'naked assertion[ ] devoid of … factual enhancement' that cannot survive a motion to dismiss." 868 F.3d at 717. Without additional factual allegations, the Court can have "no idea how" Marriott allegedly breached, and is left with "the mere possibility of misconduct," which is not enough under *Iqbal* and *Twombly*. *Id.*

Second, Plaintiffs fail to plausibly allege damages. In Nevada and California, the standard for pleading negligence damages is more stringent than Article III. Plaintiffs must allege an existing injury. Allegations of "imminent" or "certainly impending" injury "flowing from potential

fraud and identity theft" and "continued risk to … personal data" are "too tenuous.'[6] Here, as detailed above, Plaintiffs have not alleged misuse of their personal information, or any concrete harm. To the extent Springmeyer relies on money allegedly spent on credit monitoring, that argument fails for the same reasons it does not constitute an Article III injury: The threat of identity theft here is speculative, and the monitoring expenses are self-imposed—particularly because Marriott offered free monitoring services. *See Corona v. Sony Pictures Ent., Inc.*, No. 14-CV-09600, 2015 WL 3916744, at *4 (C.D. Cal. June 15, 2015); *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 961 (D. Nev. 2015).[7] Plaintiffs do not even allege that they visited Marriott's online self-service portal, which allows affected guests to determine what categories of their information were accessed, before they purchased monitoring services or before they sued—suggesting that Springmeyer's spending was driven by litigation, not privacy concerns.[8]

2. The Economic Loss Doctrine Bars Plaintiffs' Claims.

The economic loss doctrine also bars the negligence and negligence *per se* claims. "In Nevada, the economic loss doctrine bars negligent tort actions where the plaintiff seeks to recover only economic loss." *Gaming v. Trustwave Holdings, Inc.*, No. 15CV02464, 2016 WL 5799300, at *4 (D. Nev. Sept. 30, 2016). "[U]nless there is personal injury or property damage, a plaintiff may not recover in negligence for economic losses." *Terracon Consultants W., Inc. v. Mandalay Resort Grp.*, 125 Nev. 66, 74 (2009). Springmeyer has not alleged any damage to her person or to

[6] *Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226, 1232 (D. Nev. 2020), *appeal docketed*, No. 20-15460 (9th Cir. Mar. 18, 2020); *see In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 962-63 (S.D. Cal. 2012) (although plaintiffs "alleged enough to assert Article III standing to sue based on an increased risk of future harm, the Court finds such allegations insufficient to sustain a [California] negligence claim"); *Aguilar v. Hartford Accident & Indemn. Co.*, No. CV 18-8123-R, 2019 WL 2912861, at *2 (C.D. Cal. Mar. 13, 2019).

[7] While Plaintiffs assert that a year is insufficient, Springmeyer is still within the year of free coverage and has not shown she will continue to incur any monitoring costs after a year.

[8] A link the self-service portal is included in the guest notification. *Marriott International: Incident Notification*, mysupport.marriott.com (last updated June 29, 2020); *see* FAC ¶ 23.

her property. So, her negligence claims cannot proceed.

In California as well, "tort recovery of economic damages is barred unless such damages are accompanied by … physical harm (i.e., personal injury or property damage)." *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 961 (S.D. Cal. 2012). While an exception exists for "special relationship[s]," the relationship here is a standard commercial relationship. Because Lopez has not pled a relationship "beyond those envisioned in everyday consumer transactions," the economic loss doctrine applies. *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 969 (S.D. Cal. 2014).

3. Negligence *Per Se* Is Not A Cause Of Action Under California Law.

Lopez's negligence *per se* claim also must be dismissed because negligence *per se* is not an independent cause of action in California. *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, No. 19-CV-2284, 2020 WL 2214152, at *4 (S.D. Cal. May 7, 2020).

C. Plaintiffs' Breach Of Contract And Breach Of Implied Contract Claims Fail.

1. Plaintiffs Have Not Alleged A Breach Of Contract.

Count Three, for breach of contract, requires (1) the existence of a valid contract, (2) a breach by the defendant, and (3) damage as a result of the breach." *Contreras v. Am. Fam. Mut. Ins. Co.*, 135 F. Supp. 3d 1208, 1224 (D. Nev. 2015); *see also Oasis W. Realty, LLC v. Goldman*, 51 Cal. 4th 811, 821 (2011). Plaintiffs fail to plead each of these elements.

First, "[c]ourts have routinely held that a corporate privacy policy is not enforceable" unless incorporated into "some underlying contract." *Dolmage v. Combined Ins. Co. of Am.*, No. 14 C 3809, 2017 WL 5178792, at *5 (N.D. Ill. Nov. 8, 2017). No such underlying contract exists here. The Privacy Statement itself cannot be a standalone contract because contract formation requires mutual assent. *Mireskandari v. Daily Mail & Gen. Tr. PLC*, No. 12CV02943, 2013 WL 12114762, at *18 (C.D. Cal. Oct. 8, 2013); *accord Alter v. Resort Properties of Am.*, 130 Nev.

1148 (2014). Here, Plaintiffs do not claim they ever saw, read, or agreed to the privacy policy's terms. So, there was no mutual assent. *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1332 (N.D. Ga. 2019); *In re Anthem*, 162 F. Supp. 3d at 980. Nor do Plaintiffs gain by asserting they "entrusted" information to Marriott. FAC ¶ 15. They provided their information "as a means for completing [a] transaction for the purchase of [services]," not because Marriott was "offering a service to protect Plaintiffs' PII." *In re Zappos.com, Inc.*, No. 2357, 2016 WL 2637810, at *6 (D. Nev. May 6, 2016), *rev'd on other grounds*, 888 F.3d 1020 (9th Cir. 2018). Certainly, Plaintiffs have not plausibly alleged Marriott was offering a service to protect their information *from franchise employees at Marriott hotels*.

Second, Plaintiffs have not pled breach, for reasons already explained. They allege Marriott breached a contract by "fail[ing] to use reasonable organizational, technical, procedural, and administrative measures." FAC ¶ 127. The privacy policy, however, states only that Marriott will "seek" to "use reasonable [security] measures"[9]—and cautions that "no data transmission or storage system can be guaranteed to be 100% secure" and "compromise[s]" are possible. FAC ¶ 30, n.3; *supra* at 2 n.1. Particularly with this caveat, the privacy statement does *not* promise "reasonable" security measures, and statements of what a company "seek[s]" to do are "aspirational generalizations" "consistently held to be inactionable." *Vale*, 2017 WL 1102666, at *21; *accord Kuhns*, 868 F.3d at 717; *Jackson*, 2019 WL 6721637, at *2. Because Plaintiffs do not allege that Marriott did not *seek* to use reasonable measures, they have not stated a claim.[10]

[9] Marriott Group Global Privacy Statement as of Mar. 20, 2020, http://web.archive.org/web/20200328180639/https://www.marriott.com/about/privacy.mi.

[10] Plaintiffs also suggest that Marriott breached the privacy policy by "disclosing" customer data to "unauthorized third parties." Marriott, however, did not "disclose" Plaintiffs' data in the incident. The data was accessed improperly by franchise employees.

2. Plaintiffs Have Not Alleged A Breach Of Implied Contract.

Plaintiffs' implied contract claim fails for similar reasons. An "ascertainable agreement" is required to state a claim for breach of implied contract, *Mizrahi v. Wells Fargo Home Mortg.*, No. 09-CV-01387, 2010 WL 2521742, at *3 (D. Nev. June 16, 2010), which "requires … the same elements necessary [for] an express contract." *Corona*, 2015 WL 3916744, at *6. Here, Plaintiffs do not plead an "ascertainable agreement." They do not give any details of the alleged implied contract—either its terms or when and how the parties exchanged promises. Moreover, Plaintiffs again claim that the contract consisted of their "reasonable expectation that Marriott's data and cyber security practices and policies were reasonable and consistent with industry standards." FAC ¶ 132. But again, Plaintiffs allege no well-pled facts showing that Marriott's procedures were unreasonable or inconsistent with industry standards.

D. The Unjust Enrichment Claim Must Be Dismissed.

Plaintiffs next claim, unjust enrichment, "exists when the plaintiff confers a benefit on the defendant, the defendant appreciates such benefit, and there is 'acceptance and retention by the defendant of such benefit under circumstances such that it would be inequitable for him to retain [it] without payment.'" *Certified Fire Prot. Inc. v. Precision Constr.*, 128 Nev. 371, 381 (2012)); *see Hernandez v. Lopez*, 180 Cal.App.4th 932, 938 (2009). This claim also fails.

First, a claim for unjust enrichment exists only when a contract does not. *See Certified Fire Prot. Inc.*, 128 Nev. at 380; *Hernandez*, 180 Cal. App. 4th at 938. Hence, to maintain a claim for unjust enrichment where a "contractual relationship" is alleged "*requires* an allegation that the contract is invalid and unenforceable." *See Attias*, 365 F. Supp. 3d at 25 (emphasis added); *see also In re Sony*, 996 F. Supp. 2d at 984 (dismissing because "Plaintiffs do not argue that the agreements are somehow invalid or otherwise unenforceable"). Here, Plaintiffs make no such claim. For its part, Marriott's argument is that the Privacy Statement is not a contract (or was not

violated)—not that the Privacy Statement is an invalid or unenforceable contract. This rule thus requires dismissal.

Second, Plaintiffs do not identify what "benefit" they conferred that would be "unjust" for Marriott to retain simply because Plaintiffs' data was improperly accessed (but not misused) by two franchise employees. Plaintiffs say Marriott "commit[ted] to maintain [the] privacy and confidentiality" of their information, and that, otherwise, Plaintiffs would not have "transferred to and untrusted [sic] with Marriott" their information. FAC ¶ 141. But as Marriott has explained, it did not promise that no compromise was possible, nor commit to any measure it failed to implement. *See Kuhns*, 868 F.3d at 718 (dismissing unjust enrichment claim because "we are left to guess" how defendant "failed to take 'industry leading' … measures"). Certainly, Marriott did not promise that a franchise employee would never improperly access basic guest information, such as names or addresses. Nor, again, have Plaintiffs pled any facts showing that they would not have stayed with Marriott, or would somehow have paid less, had they known of this risk. Courts have rejected unjust enrichment claims where, as here, plaintiffs failed to allege that any "specific portion of" their payments "went toward data protection." *Id*; *see Gordon v. Chipotle Mexican Grill, Inc.*, 344 F. Supp. 3d 1231, 1249 (D. Colo. 2018); *Irwin v. Jimmy John's Franchise, LLC*, 175 F. Supp. 3d 1064, 1071-72 (C.D. Ill. 2016). This case is easier because Plaintiffs have not pled what they would have done differently *at all*.

E. Plaintiffs' Breach Of Confidence Claims Fail.

Under both Nevada and California law, Plaintiffs' breach of confidence claims fail.

1. Springmeyer Fails To State A Nevada Breach Of Confidence Claim.

A Nevada "breach of confidence" claim "is similar to a breach of fiduciary duty." *Frudden v. Pilling*, 842 F. Supp. 2d 1265, 1281 (D. Nev. 2012), *rev'd*, 742 F.3d 1199 (9th Cir. 2014). "[S]uch claims," however, "arise only in the context of special familial, professional, or social

confidences not arising to a technical fiduciary relationship." *Id.* The duty stems from one party "gain[ing] the confidence of the other" and "purport[ing] to act or advise with the other's interests in mind." *Atherton Res., LLC v. Anson Res. Ltd.*, No. 17CV00340, 2019 WL 78945, at *6 (D. Nev. Jan. 2, 2019). Springmeyer's breach of confidence claim must be dismissed because she alleges merely a standard commercial relationship, not a special relationship of confidence or anything approaching fiduciary duty.

2. Lopez Fails To State A California Breach Of Confidence Claim.

California breach-of-confidence claims resemble trade secret or copyright claims. A claim "arise[s] when *an idea*, whether or not protectable, is offered to another in confidence, and is voluntarily received … in confidence with the understanding that it is not to be disclosed …, and it is not to be used … for purposes beyond the limits of the confidence without the offeror's permission." *Tele-Count Eng'rs, Inc. v. Pac. Tel. & Tel. Co.*, 168 Cal. App. 3d 455, 462 (1985) (emphasis added). Although some courts describe the first element as requiring only "confidential and novel information," this phrase still means something akin to a trade secret or other intellectual property. *See Ent. Rsch. Grp., Inc. v. Genesis Creative Grp., Inc.*, 122 F.3d 1211, 1227 (9th Cir. 1997) (design of inflatable costumes could not support a claim). Here, Lopez alleges he entrusted Marriott with personal information, not an idea, and that information is nothing like a trade secret. FAC ¶¶ 3, 156. Hence, Lopez's claim fails. *See supra* Part I.A.2.[11]

F. Lopez Does Not State A California Unfair Competition Law Claim.

In Claims 8 and 9, Lopez alleges violations of the California Unfair Competition Law

[11] Breach of confidence is also an intentional tort. No California court has recognized a breach of confidence claim based on negligence. *See Reed v. NFL*, No. CV 15-01796, 2015 WL 13333481, at *2 (Sept. 24, 2015) (alleging the NFL "stole" plaintiff's idea for a TV show); *Entm't Research Grp., Inc.*, 122 F.3d at 1215 (alleging defendant "secretly entered into an agreement" with plaintiff's competitor to provide the competitor with plaintiff's designs so defendant could "get itself a better deal). For this reason too, Lopez's claim fails.

("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq*. These claims fail.

1. Lopez Lacks Statutory Standing.

First, Lopez lacks statutory standing. The UCL is "more restrictive" than Article III. *Kwikset Corp. v. Super. Ct.*, 51 Cal. 4th 310, 322-24 (2011). It limits standing to "any 'person who has suffered injury in fact and has lost *money or property'* as a result of unfair competition"—*i.e.*, "economic injury." *Id.* (emphasis added). Moreover, the injury must be "concrete," and "hypothetical or conjectural damages … are insufficient." *Mason v. Mach. Zone, Inc.*, 140 F. Supp. 3d 457, 464 (D. Md. 2015), *aff'd*, 851 F.3d 315 (4th Cir. 2017). In cases involving personal information, California courts have specifically found that a "heightened risk of identity theft, time and money spent on mitigation of that risk, and property value in one's information" all are insufficient alleged injuries. *Sony*, 903 F. Supp. 2d at 966 (collecting cases); *see In re Facebook Privacy Litig.*, 572 F. App'x 494 (9th Cir. 2014) (dismissing diminished-value claims); *Ruiz v. Gap, Inc.*, No. 07-5739, 2009 WL 250481, at *4 (N.D. Cal. Feb. 3, 2009) (dismissing monitoring-cost claims), *aff'd*, 380 F. App'x 689 (9th Cir. 2010).

Lopez alleges the same injuries already rejected as a basis for UCL standing in *Sony* and many other cases. FAC ¶¶ 69(f) (heightened risk), 69(g), (i) (time spent on mitigation), 69(h) (property value).[12] In fact, Lopez's claim is even weaker since he does not allege spending money on mitigation. *Ruiz*, 2009 WL 250481, at *4 (dismissing claims based on monitoring time/costs).[13]

[12] Some courts have accepted well-pleaded benefit-of-the bargain claims as a basis for UCL standing, but only in the rare case where plaintiffs can demonstrate that they "surrender[ed] in a transaction more, or acquire[d] in a transaction less, than he or she otherwise would have." *Kwikset*, 51 Cal. 4th at 323. Plaintiffs have failed to make that showing. *See supra* Part I.A.2.

[13] Courts have even dismissed claims brought under the UCL where data was in fact misused, unless there were real economic losses. *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, No. 316CV00014GPCBLM, 2016 WL 6523428 (S.D. Cal. Nov. 3, 2016).

2. Lopez Has Failed To State An Unfair Competition Law Claim.

Lopez claims Marriott violated the UCL because its conduct was either "unlawful" or "unfair." *See Aryeh v. Canon Bus. Sols., Inc.*, 55 Cal. 4th 1185, 1196 (2013). Both claims fail.

Unlawful. The UCL "borrows violations of other laws and treats them as unlawful practices' that the unfair competition law makes independently actionable." *Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (1999). Lopez alleges that Marriott's conduct was "unlawful" because California's data breach statute required Marriott to "implement and maintain reasonable security procedures and practices." Cal. Civ. Code § 1798.81.5(b); FAC ¶ 169. Lopez also alleges that California's data breach statute required Marriott to:

> disclose a breach of the security system … to a resident of California … whose unencrypted personal information was … acquired by an unauthorized person … in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement … or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Cal. Civ. Code § 1798.82; *see* FAC ¶ 170.

This claim fails, first, because California's data breach statute does not apply. That statute applies only to "personal information," which is defined as either:

> (A) "[a]n individual's first name or first initial and the individual's last name in combination with" "a social security number," "driver's license number," other numbers "commonly used to verify the identity of a specific individual," "account number or credit or debit card number, in combination with any required security code, access code, or password," medical information, health insurance information, or "[u]nique biometric data", or
>
> (B) "[a] username or email address in combination with a password or security question and answers that would permit access to an online account."

Id. § 1798.81.5(d)(1). Lopez does not allege the disclosure of any such information.

Lopez's "unlawful practices" claim also fails for the same reason as the negligence claim: He alleges no facts identifying what Marriott's security practices were or how they were deficient—absences that are particularly glaring given that the information was accessed by

insiders, not in a data breach. Also absent are any facts suggesting Marriott did not disclose the incident in a "timely and accurate" manner. The disclosure—whose accuracy Lopez concedes—went to 5.2 million accounts within one month and five days of Marriott learning of possible unauthorized access, which easily meets the statute's timing requirement. *Id.* § 1798.82(a) (requiring disclosure in "most expedient time possible … consistent with [the] legitimate need[] … to determine the scope of the breach and restore reasonable integrity of the data system").

Unfair. "'Unfair' conduct must be tethered to some legislatively declared policy or have some effect on competition," or be "immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers." *Hernandez v. Wells Fargo & Co.*, No. C 18-07354, 2019 WL 2359198, at *5 (N.D. Cal. June 3, 2019) (internal quotations omitted).[14] Plaintiffs satisfy neither test.

First, Lopez does not identify any legislative policy to which his "unfair practices" claim is "tethered." If anything, the Complaint shows that this claim *does not* implicate any legislative policy. When California decided what disclosures of personal information would be actionable, it excluded the type of information at issue here. Second, Lopez claims that Marriott's practices were "substantially injurious" because they "deceive[d] the public into believing their PII was securely stored, when it was not." FAC ¶ 176. But as Marriott has explained, Lopez has not pled any facts supporting the assertion that Marriott used "sub-standard … practices." *Id.* Furthermore, it told Plaintiffs and the public that, while it "seek[s] to use reasonable [security] measures," "no data transmission or storage system can be guaranteed to be 100% secure" and "compromise[s]" were possible. In *In re Sony*, the court dismissed a nearly identical "unfair" practices claim. 903 F. Supp. 2d at 967. The plaintiff alleged Sony had misrepresented its practices—but Sony's privacy policy

[14] Lopez's claims are subject to Rule 9(b)'s heightened pleadings standards because they are grounded in a claim of misrepresentation. *See In re Sony*, 903 F. Supp. 2d at 967.

underscored that "there is no such thing as perfect security" and "we cannot ensure or warrant the security of any information." *Id.* at 968. This "clear admonitory language" meant that "no reasonable consumer could have been deceived." *Id.* The same is true here.

G. Lopez Does Not State A California Consumer Privacy Act Claim.

In Claim 10, Lopez asserts a violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150(a). Under the Privacy Act:

> Any consumer whose nonencrypted and nonredacted *personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5*, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action.

Id. (emphasis added). Hence, the Privacy Act also applies only to "personal information" as defined in § 1798.81.5(d)(A)(1)—which, again, is not at issue here. Lopez's claim therefore fails.

This claim also fails because the Privacy Act requires a consumer bringing an "individual or class-wide" action to first "provide[] a business 30 days' written notice identifying the specific provisions … the consumer alleges have been or are being violated." Cal. Civ. Code § 1798.150. Lopez does not allege he ever provided such notice (and he did not). *Cf. Ruszecki v. Nelson Bach USA Ltd.*, No. 12-cv-495, 2015 WL 67509080, at *5 (S.D. Cal. June 25, 2015) (dismissing California Consumer Legal Remedies Act claims where plaintiff failed to give statutory notice).[15]

H. Springmeyer Does Not State A Nevada Deceptive Trade Practices Act Claim.

Claim 11 alleges a violation of the Nevada Deceptive Trade Practices Act, which prohibits

[15] While an "individual consumer" may initiate "an action solely for actual pecuniary damages without providing notice," *see* Cal. Civ. Code § 1798.150(b), Lopez is not seeking "solely" actual pecuniary damages and indeed has not identified *any* "pecuniary damages." Lopez also cannot seek injunctive relief because he has not demonstrated "a sufficient likelihood that [he] will again be wronged in a similar way," by having his data improperly accessed again in the future. *Villa v. Maricopa Cty.*, 865 F.3d 1224, 1229 (9th Cir. 2017). Hence, dismissal in full is required.

"knowingly making a false representation" regarding a good or service, advertising "goods or services with intent not to sell" as advertised, failing to disclose a "material fact," and violating "a state or federal statute or regulation relating to the sale … of goods or services." Nev. Rev. Stat. §§ 598.0915, .0923. Rule 9(b) applies. *Bank of N.Y. Mellon v. Sierra Ranch Homeowners Ass'n*, No. 15CV1914, 2017 WL 3174904, at *5 (D. Nev. July 26, 2017), *appeal docketed*, No. 17-16713 (9th Cir. Aug. 25, 2017).

Springmeyer provides a conclusory laundry list of supposed failures, misrepresentations, omissions, and statutory and common law violations, all relating to the alleged failure to provide "reasonable" security. FAC ¶ 191(a)-(c). But as Marriott has explained, these claims fail under Rule 8—and so necessarily fail under Rule 9(b). Springmeyer alleges a failure to "implement and maintain reasonable security and privacy measures." *Id.* ¶ 191(d)-(e). But she says not a word about what measures Marriott took, how they were deficient, or how alternatives would have prevented the incident. Springmeyer also alleges a series of misrepresentations but ignores Rule 9(b)'s requirement to provide the "time, place, and contents." *Harrison v. Westinghouse Savannah River Co.*, 176 F.3d 776, 784 (4th Cir. 1999). Springmeyer's alleged "omissions" are merely restatements of the alleged misrepresentations, and assert that Marriott "did not reasonably … secure … PII" or "did not comply with common law and statutory duties." FAC ¶ 191(f)-(g). As Marriott has shown, Springmeyer has pled no specific facts to support these naked assertions.

I. A Declaratory Judgment Is Not Appropriate.

Plaintiffs' sixth "claim" is a request for a declaratory judgment. A declaratory judgment, however, is a "remedy, not a substantive cause of action." *ACA Fin. Guar. Corp. v. City of Buena Vista*, 298 F. Supp. 3d 834, 843 (W.D. Va. 2018), *aff'd*, 917 F.3d 206 (4th Cir. 2019). Where, as here, a plaintiff's "substantive claims fail … so must its Declaratory Judgments Act claim." *CGM*,

LLC v. BellSouth Telecomms., Inc., 664 F.3d 46, 56 (4th Cir. 2011).[16]

III. Plaintiffs Lack Standing To Bring Claims On Behalf Of A Nationwide Class.

Any claims that survive this Motion must be narrowed to Plaintiffs' states of residence. To have standing to represent absent class members, a plaintiff must allege "a distinct and palpable injury to himself" that he shares with those other class members. *Zaycer v. Sturm Foods, Inc.*, 896 F. Supp. 2d 399, 408 (D. Md. 2012) (dismissing class action claims for states lacking a named plaintiff). Hence, a single plaintiff cannot "bring a class action complaint under the laws of" each of the fifty states unless he can allege that he has suffered a "concrete, particularized injuries relating to [each] state.'" *Mayor & City Council of Balt. v. Actelion Pharm., Ltd.*, No. CV GLR-18-3560, 2019 WL 4805677, at *8 (D. Md. Sept. 30, 2019), *appeal docketed*, No. 19-2233 (4th Cir. Nov. 5, 2019). This rule protects absent class members by ensuring that the named plaintiff shares their injury. *See In re Graphics Processing Units Antitrust Litig.*, 527 F. Supp. 2d 1011, 1026 (N.D. Cal. 2007). It also protects defendants from being "dragged … into expensive nationwide class discovery" in nearly every class action, "potentially without a good-faith basis." *Actelion Pharm., Ltd.*, 2019 WL 4805677, at *8.

Here, each putative class members' claims will be governed by the laws of the state where they reside, not the laws of Maryland. *See supra* Part II.A. Because Springmeyer and Lopez lack claims under any state's law other than Nevada and California, the nationwide claims must be dismissed. *See Hassan v. Lenovo*, No. 18-cv-105, 2019 WL 123002, at *2 (E.D.N.C. Jan. 7, 2019).

CONCLUSION

For the reasons stated above, Marriott's Motion to Dismiss should be granted.

[16] Even if any of Plaintiffs' claims survived, the declaratory judgment claim would have to be dismissed. A declaratory judgment is meant to permit "'prospective defendants to sue to establish their nonliability,' not create a substantive tack-on claim for an already-existing plaintiff who is adjudicating an already-live legal issue." *ACA*, 298 F. Supp. 3d at 843.

Paul B. Rietema (*pro hac vice*)
Jenner & Block LLP
353 N. Clark St.
Chicago, Illinois 60654
Telephone: (312) 840-7208
Facsimile: (312) 840-7308
prietema@jenner.com

/s/ David W. DeBruin

David W. DeBruin (Bar No. 07757)
Lindsay C. Harrison (*pro hac vice*)
Zachary C. Schauf (*pro hac vice*)
Jenner & Block LLP
1099 New York Ave. NW, Suite 900
Washington, DC 20001
Telephone: (202) 639-6865
Facsimile: (202) 639-6066
ddebruin@jenner.com
lharrison@jenner.com
zschauf@jenner.com

Attorneys for Defendant

CERTIFICATE OF SERVICE

I hereby certify that on August 6, 2020, the foregoing, with exhibits thereto, was filed with the Clerk of Court using CM/ECF, which will send notification to the registered attorneys of record that the document has been filed and is available for viewing and downloading.

/s/ David W. DeBruin
Attorney for Defendant